

**REMARKS**

Reconsideration of this application, as presently amended, is respectfully requested. Claims 1-23 are pending in this application. Claims 1-23 stand rejected.

Applicants would like to thank Examiner Doan and the Examiner's supervisor for the courtesies extended to applicants' representative during the telephonic interview conducted on December 4, 2007. During the course of the interview, the rejection under §102 in view of **Nakajima** (US Pub No. 2003/0169714) was discussed, with emphasis on the differences between the invention recited in claims 1 and 16 and the **Nakajima** reference. No agreement was reached during the interview.

**Claim Rejection-35 U.S.C. 102**

Claims 1-23 are rejected under 35 U.S.C. §102(e) as being anticipated by **Nakajima** (US Pub No. 2003/0169714, previously cited). For the reasons set forth in detail below, this rejection is respectfully traversed.

**The invention as recited in claim 1**

Claim 1 recites a method for automatically identifying an access right to **protected areas in a first network** using a unique connection identifier of a second network, comprising the following procedural steps:

dynamic or static assignment of a unique identifier of the first network for a terminal, during or prior to the latter's connection to the first network by means of the second network;

**storage of a combination of at least the unique connection identifier of the second network by means of which the connection was made, and the unique identifier of the first network in an authentication unit** [emphasis added];

**a provider of the protected area requesting** [emphasis added] the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area;

authenticating (only) **the unique connection identifier of the second network** [emphasis added] and/or communicating (only) **the unique connection identifier of the second network** [emphasis added] to the provider of the protected area by means of the authentication unit;

checking whether an access right for the protected area exists for the unique connection identifier of the second network.

In the following discussion, the features of claim 1 will be described for a better understanding of the claimed subject matter in accordance with a specific example such as accessing a service in the internet via a telephone connection. The internet would represent the first network according to claim 1, in which a typical **unique identifier is the IP address**. The telephone connection would represent the second network according to claim 1. The second network has for example the **telephone number as a unique connection identifier**.

As will be discussed in detail below, it is respectfully submitted that **Nakajima** does not disclose or suggest the following features recited in claim 1.

First, it is submitted that **Nakajima** does not disclose or suggest the claimed “a provider of the protected area requesting the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area.”

The Office Action (1) considers the Internet 104 to correspond to the claimed “first network; (2) considers the mobile communication network 100 to correspond to the claimed “second network”; (3) considers the telephone number of the mobile terminal 105 to correspond to the claimed “unique connection identifier of the second network”; and (4) considers the IP address for accessing the Internet 104 via the service gateway 102 to correspond to the claimed “unique identifier of the first network.”

Unlike the claimed invention, according to **Nakajima**, when the terminal 105 would like to access the Internet 104 (i.e., access the protected area), the mobile terminal 105 transmits a service request to the subscriber system 103, which includes the authentication unit 210, to have the authentication unit 210 authenticate the service request (see paragraphs 0037) and [0038]). The service request includes an ID number and the IP address of the service terminal 101, and a network identification code (i.e., serial number) and the telephone number of the mobile terminal 105. Thus, firstly, in contrast to the claimed invention, **Nakajima et al.** teaches that the mobile terminal 105 “requests” authentication of its service request, and does not disclose or suggest that “a provider of the protected area [in the first network]” sends any sort of request to the authentication unit 210.

Secondly, unlike the claimed invention, the authentication unit does not “determine the unique connection identifier of the second network using the unique identifier of the first network.” If the **Nakajima** reference were to disclose this feature, then the authentication unit 210 would determine the telephone number of the mobile terminal (i.e., the unique connection identifier of the second network) by using the IP address of the Internet 104 (i.e., the unique identifier of the first network).

However, unlike the claimed invention, the authentication unit 210 of **Nakajima et al.** does *not use* the IP address to determine the telephone number of the mobile terminal 105. In contrast to the claimed invention, the telephone number of the mobile terminal 105 is used to determine whether the IP address is to be sent to a service gateway 102. More specifically, the authentication unit 210 of **Nakajima et al.** authenticates the mobile terminal 105 (i.e., determines whether the mobile terminal is under management of the subscriber system 103) by determining whether the telephone number (unique connection identifier) and a network identification code (i.e., serial number) of the mobile terminal 105 included in the service request are stored in a subscriber database (see paragraph [0038] and step S303). If the telephone number of the mobile terminal 105 and the network identification code (i.e., serial number) of the mobile terminal 105 included in the service request are stored in a subscriber database, then the mobile terminal is authenticated and the authentication unit 210 sends the IP address to a service gateway as a service delivery point. Thus, unlike the claimed invention, the IP address (unique identifier of first network) is simply part of the service request, and is not used by the

authentication unit 210 to determine the telephone number (unique connection identifier of second network) of the mobile unit 105.

Moreover, in contrast to the claimed invention, according to **Nakajima**, a single access request issued by mobile phone 105 is issued and after authentication, access to the requested service, i.e., the Internet, is allowed. Contrary to the Examiner's assertion, **Nakajima** does not teach a service provider of a protected area requesting the authentication unit to determine the unique connection identifier of the second network using the unique identifier of the first network when the terminal would like access to the protected area, as claimed. The authentication unit in **Nakajima** determines once, whether both unique connection identifiers which are transmitted thereto by the mobile unit 105 are stored in a subscriber database, to authenticate the service request issued by the mobile unit, as for example described in paragraphs [0034] and [0035] of **Nakajima**.

At no point in time does the authentication unit 210 determine the unique connection identifier of the second network using the unique identifier of the first network upon request of a service provider, when the terminal would like access to the protected area. The above feature of the claimed invention allows the terminal to access protected areas in the second network, such as a pay TV-channel etc, after connecting to the first network and after an authentication request is issued to the authentication unit by the service provider. It should be noted, that **Nakajima** relates only to accessing the first network, which is a prerequisite in the method of the present invention, which specifically relates to accessing "further" protected areas in the first network upon an authentication request by the respective service provider. **Nakajima** neither shows nor

even remotely suggests such an access to a “further” protected area in the first network, i.e., the Internet, upon an authentication request of a service provider.

Furthermore, it is submitted that **Nakajima et al.** does not disclose or suggest “storage of a combination of at least the unique connection identifier of the second network by means of which the connection was made, and the unique identifier of the first network in an authentication unit.” Contrary to the Examiner’s assertion, this feature is not disclosed by **Nakajima**. In **Nakajima**, the authentication unit does not store said combination, but only once checks the combination and then authenticates access to the Internet or not. Thus, **Nakajima** does not teach **storing** the combination in the authentication unit. Indeed, since **Nakajima** teaches only a single authentication there appears to be no need to store the combination, as claimed in claim 1.

Moreover, applicant respectfully submits that it is inherent in claim 1 that the authentication unit stores the identifiers for an extended period, as they are stored upon accessing the first network and have to be available when a provider of the protected area requests authentication. In view of the fact that the authentication unit of claim 1 clearly has to wait for a request by a provider of the protected area..., the only **reasonable** interpretation is that the information has to be stored for an extended time period. Such extended storage as claimed, however, is not disclosed in **Nakajima**.

It is, however, this extended storage of the combination, which allows a provider of the protected area to place an appropriate request to the authentication unit, when the terminal intends to access the protected area in the first network. Again it should be stressed that the

application is clearly directed towards to identify an access right to **a protected area in a first network**, i.e., after having connected to the first network and going to a deeper level. **Nakajima** merely discloses identifying an access right to the first network itself, and neither shows nor suggests an identification at a later stage.

Claim 1 of the present invention further requires “authenticating **the unique connection identifier of the second network** and/or communicating **the unique connection identifier of the second network** to the provider of the protected area by means of the authentication unit; and checking whether an access right for the protected area exists for the unique connection identifier of the second network.”

Taking the example of the Pay-TV area in the internet, the service provider will either get an authentication with respect to the unique connection identifier of the second network (i.e. the telephone number), which case, for example, allows billing via the provider of the authentication unit, or the unique connection identifier of the second network (i.e. telephone number) is transmitted, which case for example allows billing directly to the telephone number by the service provider.

The invention in accordance with claim 16

The same arguments provided above similarly apply to independent method claim 16 which additionally comprises automatic deletion of data from the authentication unit, if a connection to at least one of the two networks is terminated. This feature additionally increases

security, inasmuch as upon termination, the authentication data are automatically deleted from the authentication unit and may thus not be misused.

This feature is clearly also not shown or disclosed in **Nakajima**, inasmuch as the authentication does not store the above combination for the duration of the connection. The data are permanently stored in the subscriber system and authenticated once in the authentication unit, but not stored therein.

In view of the above remarks, reconsideration and withdrawal of the rejection under §102 are respectfully requested.

### **CONCLUSION**

In view of the foregoing, it is submitted that all pending claims are in condition for allowance. A prompt and favorable reconsideration of the rejection and an indication of allowability of all pending claims are earnestly solicited.

If the Examiner believes that there are issues remaining to be resolved in this application, the Examiner is invited to contact the undersigned attorney at the telephone number indicated below to arrange for an interview to expedite and complete prosecution of this case.



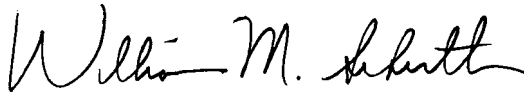
Application No. 10/539,506  
Art Unit: 1640

Request for Reconsideration under 37 C.F.R. §1.116  
Attorney Docket No.: 052703

If this paper is not timely filed, Applicants respectfully petition for an appropriate extension of time. The fees for such an extension or any other fees that may be due with respect to this paper may be charged to Deposit Account No. 50-2866.

Respectfully submitted,

**WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP**

A handwritten signature in black ink, appearing to read "William M. Schertler". The signature is fluid and cursive, with the first name "William" and last name "Schertler" being clearly legible.

William M. Schertler  
Attorney for Applicants  
Registration No. 35,348  
Telephone: (202) 822-1100  
Facsimile: (202) 822-1111

WMS/dlt